(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 195 27 715 A 1**

(51) Int. Cl.[6]:
H 04 L 9/32
H 04 L 29/12
G 07 C 9/00
H 04 Q 7/34

(21) Aktenzeichen: 195 27 715.5
(22) Anmeldetag: 31. 7. 95
(43) Offenlegungstag: 6. 2. 97

DE 195 27 715 A 1

(71) Anmelder:
DeTeMobil Deutsche Telekom MobilNet GmbH, 53227 Bonn, DE

(74) Vertreter:
Riebling, P., Dipl.-Ing. Dr.-Ing., Pat.-Anw., 88131 Lindau

(72) Erfinder:
Kröber, Markus, Dipl.-Ing., 53225 Bonn, DE; Kaliner, Stefan, Dipl.-Ing., 53123 Bonn, DE

(56) Entgegenhaltungen:
DE 42 42 151 C1
DE 41 38 861 A1
EP 5 52 392 A1
DE-Z.: DECHAUX, C. et al.: Was bedeuten GSM und DCS? In: Elektrisches Nachrichtenwesen, 2. Quartal 1993, S.118-127;
DE-Z.: WATTS, A.: Datenverschlüsselung in der Chipkarte. In: Elektronik 22, 1994, S.88-94;

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Verfahren zur Nutzeridentifikation und -authentifikation bei Datenfunkverbindungen, zugehörige Chipkarten und Endgeräte

(57) Beschrieben wird ein Verfahren zur Nutzeridentifikation bei Datenfunk-Verbindungen, wobei die zur Nutzeridentifikation erforderlichen Daten auf einem gesonderten Datenträger getrennt von einem Endgerät abgelegt werden. Die Nutzeridentifikation wird durch Kommunikation zwischen Datenträger und Endgerät durchgeführt.

DE 195 27 715 A 1

Beschreibung

Die vorliegende Erfindung beschäftigt sich mit einem Verfahren zur Nutzeridentifikation und -authentifikation bei Datenfunk-Verbindungen sowie mit den zugehörigen Einrichtungen, insbesondere mit Chipkarten und Endgeräten.

Datenfunk-Verbindungen unterscheiden sich grundlegend von GSM (Global System for Mobile Communication) das bereits seit längerem in Betrieb ist. GSM stellt einem gemeinsamen Standard bereit und erlaubt daher die Verwendung eines Endgerätes in unterschiedlichen Netzen.

Ein wesentlicher Unterschied zwischen Datenfunk und GSM besteht in der Art der Verbindung während der Datenübertragung. So wird bei GSM stets die Verbindung zu dem Gesprächspartner aufrechterhalten, auch wenn keine Daten übermittelt werden. Dies ist bei Datenfunk nicht der Fall. Hier werden die Daten in Form von Datenpaketen übertragen; nur für den Zeitraum dieser Übertragung existiert eine gebührenpflichtige Verbindung.

Ein weiterer Unterschied liegt in der Art der übermittelten Daten und den Gesprächspartnern. GSM wird fast ausschließlich zur Übertragung von Sprache verwendet, während Datenfunk nicht für die Übertragung von Sprache konzipiert ist, sondern für die Kommunikation zwischen Endgeräten, also typischerweise zwischen zwei Rechnereinheiten.

Die Identität des Benutzers wird bei GSM über eine personenbezogene Karte überprüft und sichergestellt. Hierbei werden zu Datenprüfung verschiedene Informationen an eine Feststelle bzw. einen Zentralrechner übertragen. Dieser nimmt die Überprüfung der Daten vor und bestätigt die Kompetenz des Benutzers bzw. verweigert die Nutzung.

Demgegenüber ist bei Datenfunk ein benutzerspezifisches Endgerät vorgesehen. Die identifizierenden Daten werden während der Produktion beim Endgerätehersteller eingebracht und sind danach nicht oder nur in einem sicherheitskritischen Vorgang unter Verwendung spezieller Programmierwerkzeuge veränderbar. Im Falle eines Defekts und eines damit verbundenen Gerätewechsels müssen die Rufnummer gewechselt und das Teilnehmerverzeichnis erneuert werden. Die temporäre Verknüpfung eines Gerätes mit verschiedenen Teilnehmern ist nicht möglich.

Die Verteilung der Teilnehmerverhältnisse bzw. die Zuordnung der Rufnummern erfordert eine enge Abstimmung zwischen dem Betreiber eines Mobilfunknetzes und den Endgeräteherstellern. Insbesondere entzieht sich der sicherheitskritische Vorgang der Einbringung der identifizierenden Daten in das Endgerät der Kontrolle des Netzbetreibers.

Zusätzlich entstehen logistische Probleme, da in der Regel die Rufnummern der Teilnehmer gebietsbezogen vergeben werden. Es muß also bereits bei der Herstellung bzw. Fertigstellung und Auslieferung eines Endgerätes bekannt sein, in welchem Gebiet der Benutzer das Gerät betreiben möchte.

Eine einfache Übertragung des Identifikationssystems, das bei GSM genutzt wird, ist nicht möglich. Bei Datenfunk-Netzen ist eine Zentralstelle zur Überprüfung der Teilnehmeridentität nicht vorhanden und auch weder bei der bisherigen noch bei der erfindungsgemäßen Struktur erforderlich.

Aufgabe der vorliegenden Erfindung ist es daher, ein Verfahren sowie Einrichtungen zur Nutzeridentifikation und -authentifikation bei Datenfunk bereit zustellen, die eine endgeräteunabhängige Identifizierung des Benutzers erlauben.

Erfindungsgemäß wird diese Aufgabe durch die technische Lehre von Anspruch 1 gelöst.

Wesentlich hierbei ist, daß eine Trennung der Nutzerinformation vom Endgerät stattfindet und der Benutzer sowohl mit einem Endgerät als auch mit einem Datenträger, bevorzugt in Form einer Karte oder Chipkarte, ausgerüstet wird. Anders ausgedrückt wird das Endgerät physikalisch und logisch in eine anonyme, unpersönliche Komponente und einen den Teilnehmer und dessen besondere Merkmale identifizierenden Anteil, nämlich die Karte, aufgeteilt.

Hierbei ist die Nutzeridentifikation auf der Karte abgelegt, und eine Überprüfung dieser Nutzeridentifikation erfolgt durch das Endgerät. Eine Kommunikation mit einer übergeordneten Zentralstelle zur Nutzeridentifikation ist nicht erforderlich.

Hierdurch werden mehrere Verbesserungen erzielt:
Die Teilnehmeridentität (und andere individuelle Daten) werden auf eine Chipkarte verlagert und somit das System in ein anonymes Endgerät und eine persönliche Chipkarte aufgeteilt. Diese kann dem Endgerät entnommen werden und ist uneingeschränkt mobil. Das Teilnehmerverhältnis steht daher in beliebigen Endgeräten unverändert zur Verfügung. Ein einzelnes Gerät ist durch einfachen Wechsel der Karte von beliebig vielen Teilnehmern benutzbar.

Die Programmierung der Teilnehmerverhältnisse (Personalisierung) ist von den Endgeräteherstellern unabhängig und kann vom Netzbetreiber unter vollständiger Kontrolle selbst durchgeführt werden. Eine aufwendige Kontrolle der Endgerätehersteller sowie die obenerwähnte Logistik sind nicht erforderlich.

In einer bevorzugten Ausführungsform ist die Chipkarte als Mikroprozessor-Chipkarte ausgebildet. Die Karte ist dann flexibel als mobiler Datenspeicher einsetzbar. Dies und die Möglichkeiten eines frei programmierbaren Mikroprozessorsystems erlauben die Realisierung endgeräteunabhängiger Sonder- und Komfortfunktionen.

So ist es z. B. möglich, die Berechtigung zum Netzzugang und die Nutzeridentifikation anhand von Karte und Endgerät durchzuführen, während Anwendungen, die von Dritten im Netz angeboten werden, über weitere Identifikationsverfahren geschützt werden können .. Diese Applikationen sind dann bevorzugt vom Netzbetreiber unabhängig, der lediglich die Dienstleistung der Datenübertragung zur Verfügung stellt.

So ergibt sich hier die Möglichkeit, die Chipkarte und die in der vorliegenden Erfindung bereitgestellten Kommunikationsmechanismen zur Nutzeridentifizierung und -authentifikation gegenüber der Applikation (als Zugangsberechtigung) zu nutzen.

Im folgenden wird die Erfindung in Zusammenhang mit dem Mobilfunksystem Modacom näher beschrieben. Genaue Informationen hinsichtlich des Aufbaus dieses Systems sind bei der Anmelderin erhältlich. Selbstverständlich ist der Grundgedanke der Erfindung bei beliebigen Datenfunk-Netzen einsetzbar; die Erfindung ist nicht auf Modacom beschränkt.

Die Motive für die Einführung der Chipkarte in das Mobilfunksystem Modacom sind vielfältig:
Die zur Zeit unumgängliche Personalisierung der Endgeräte mit allen ihren logistischen Nachteilen soll ersetzt werden durch eine zeitgemäße Lösung. Daneben erwartet man neue Komfortmerkmale, wie Mobilität

des Teilnehmerverhältnisses ohne Endgerät, einfachere Bereitstellung von anonymen Ersatzgeräten, sowie ggf. erhöhte Datensicherheit.

Inhalt dieser Anmeldung ist ein Konzept im Hinblick auf eine mögliche Realisierung einer Chipkarte in Modacom, ihre Architektur sowie die notwendigen Sicherheitsfunktionen.

Der Erfindungsgegenstand der vorliegenden Erfindung ergibt sich nicht nur aus dem Gegenstand der einzelnen Patentansprüche, sondern auch aus der Kombination der einzelnen Patentansprüche untereinander.

Alle in den Unterlagen, einschließlich der Zusammenfassung, offenbarten Angaben und Merkmale, insbesondere die in den Zeichnungen dargestellte räumliche Ausbildung werden als erfindungswesentlich beansprucht, soweit sie einzeln oder in Kombination gegenüber dem Stand der Technik neu sind.

Im folgenden wird die Erfindung anhand von lediglich einen Ausführungsweg darstellenden Zeichnungen näher erläutert. Hierbei gehen aus den Zeichnungen und ihrer Beschreibung weitere erfindungswesentliche Merkmale und Vorteile der Erfindung hervor.

Dabei zeigt

Fig. 1 die erfindungsgemäße Aufteilung in Chipkarte und Endgerät;

Fig. 2 unterschiedliche Ausführungsformen der Chipkarten;

Fig. 3 ein Beispiel für die logische Struktur der Chipkarte;

Fig. 4 schematisch ein Verfahren zur Authentifikation;

Fig. 5 schematisch ein Verfahren zur Datenübertragung;

Fig. 6 den Schlüsselaustausch zwischen Chipkarte und Endgerät.

Die Modacom Chipkarte im Systembezug

Von der Einführung der Chipkarte 1 sind allein die mobilen Systemkomponenten, d. h. das Modacom-Endgerät 2 mit der (evtl. PC-gestützten) Modacom Applikation 3, betroffen. Auswirkungen auf andere Systemkomponenten existieren nicht.

Das bisherige Endgerät wird physikalisch und logisch aufgetrennt in einen den Teilnehmer und dessen besondere Merkmale identifizierenden Anteil, die Chipkarte 1, und eine anonyme, unpersönliche Komponente, das neue Endgerät 2. Diese Karte 1 kann dem Endgerät 2 entnommen werden und ist in ihrer Mobilität ebenso uneingeschränkt wie der Rest des Mobilsystems. Es entsteht eine zusätzliche komplexe Schnittstelle.

Die veränderte Konfiguration des Mobilsystems (= Chipkarte 1 + Endgerät 2 + Applikation 3, siehe **Fig.** 1) bedingt eine Reihe neuer Anforderungen in einer geänderten Aufgabenverteilung zwischen den beteiligten Komponenten.

Die Modacom Chipkarte

Die Modacom Chipkarte 1 dient in der Hauptsache als mobiles Identifikationsmedium. Ein Teilnehmerverhältnis ist an den Besitz der Karte gebunden und wird durch diese identifiziert und charakterisiert. Die Karte trägt alle im Mobilsystem vorhandenen teilnehmerspezifischen Daten. Wird die Karte entnommen und in ein anderes Endgerät 2 eingesetzt, steht das Teilnehmerverhältnis unverändert zur Verfügung.

In diesem Sinne relevante Daten (vgl. "Architektur") sind:

Modacom Teilnehmeridentifizierung und Ruf-Adresse LLI, Home-Node und eventuelle Gruppenzugehörigkeiten, gekennzeichnet durch Group-IDs. Diese Daten werden in der Karte gespeichert und sind dort vor unautorisierter Veränderung geschützt.

Zusätzlich liefert die Chipkarte 1 einen flexiblen, weil wahlfrei beschreibbaren Datenspeicher, der sich zum Ablegen der verschiedensten Informationen eignet: Als Speicher für netzrelevante Informationen (z. B. für ausländische Netze), für Endgeräte-Konfigurationsdaten und auch für Konfigurationsdaten der Applikation. Diese Daten sind somit mobil und können an jedem vorhandenen Modacom-Endgerät 2 genutzt und auch geändert oder ergänzt werden.

Im Mobilsystem übernimmt die Karte 1 die Aufgabe eines Sicherheitsmodules: Die enthaltenen Daten sind vor unberechtigtem Zugriff zu schützen und im Zusammenwirken mit dem Endgerät 2 sind Mechanismen zur sicheren Datenübertragung über die Kartenschnittstelle bereitzustellen. Ein allgemeiner Zugriffsschutz wird durch die (abschaltbare) PIN-Prüfung realisiert.

Das Modacom Endgerät

Das Modacom Endgerät 2 stellt die im Hinblick auf die Chipkarte 1 notwendigen Funktionen zur Verfügung. In der Zeit zwischen Aktivierung und Deaktivierung steuert es alle Zugriffe auf die Chipkarte. Es bedient sich dazu des vorgegebenen Befehlssatzes und wertet die Antworten der Karte aus. Zur Unterstützung der Sicherheitsfunktionen speichert es die öffentlichen Schlüssel, generiert Zufallszahlen und führt kryptographische Algorithmen aus (siehe "Sicherheitsfunktionen").

Gesichert übertragene Daten werden sicher abgelegt. Es liegt in der Verantwortung des Endgerätes 2, das Sicherheitsniveau der Karte nicht zu beeinträchtigen.

Das Endgerät 2 stellt einen bidirektionalen Kanal zwischen Karte 1 und Applikation 2 bereit, über den die PIN-Funktionen (Prüfen, Ein-/Ausschalten, Ändern und Entsperren) sowie die applikationsseitige Nutzung des Kartenspeichers abgewickelt werden.

Die Modacom Applikation

Die Unterstützung bzw. Nutzung der Modacom Chipkarte 1 durch die Applikation 3 ist optional. Wenn gewünscht, steht der vom Endgerät 2 bereitgehaltene Übertragungsweg zur Verfügung, um die PIN-Funktionen zu unterstützen oder die Karte zur Speicherung von applikationsspezifischen Daten, z. B. Konfigurationsdaten zu nutzen. Die Schnittstelle zwischen Applikation 3 und Endgerät 2 ist ansonsten unbeeinflußt.

Die Technik der Modacom Chipkarte

Die Modacom Chipkarte wird in Form einer ISO-Identifikationskarte mit integriertem Mikro-Controller und EEPROM Speicher realisiert.

Die grundlegenden Anforderungen an diese Systemkomponente, insbesondere im Hinblick auf die gewünschten Sicherheitsmerkmale, erlauben den Einsatz einfacherer Speichermedien, wie etwa einer Magnetstreifenkarte oder einer simplen Speicherkarte nicht, sondern erfordern den Einsatz echter Computerleistung. Zusätzlich wird der EEPROM Speicher für die Bewahrung veränderlicher Kartendaten vorausgesetzt.

Dieser EEPROM-Speicher kann vom Benutzer teilweise selbst genutzt werden, z. B. zur Eingabe von Daten zur Verwendung in von Dritten im Netz bereitgestellten Informationen.

Es wird daher die Einführung einer Kartentechnologie vorgeschlagen, wie sie in GSM — bei vergleichbarem Anforderungsprofil — mit Erfolg eingesetzt wird.

Durch die weitestgehende Verwendung von international standardisierten Merkmalen (z. B. physikalische Schnittstellenparameter, Übertragungsprotokoll, etc.) wird einerseits die Kartenschnittstelle kompatibel zu bereits vorhandenen, beispielsweise bei DeTeMobil vorhandenen, administrativen Systemen (z. B. Personalisierungszentrum für SIMs — PCS oder Chipkarten Test- und Servicestation X13) gehalten, andererseits den Herstellern von Modacom Endgeräten eine relativ einfache — weil standardisierte — Realisierung der Kartenschnittstelle ermöglicht. Zusätzlich ergibt sich daraus eine prinzipielle Kompatibilität mit anderen gleichartig standardisierten Chipkartenanwendungen.

Die Modacom Chipkarte 1 kann gemäß Fig. 2 in zwei oder mehr Formaten realisiert werden: Als Typ ISO ID-1, (Normalgröße, entsprechend einer EC- oder Kreditkarte) gemäß den internationalen Standards ISO/IEC 7810 und 7816-1,2 sowie, zur Unterstützung kleiner Endgeräteabmessungen, als Typ CEN ID-000 (Plug-In Modul, siehe GSM) entsprechend dem europäischen Standard CEN ENV 1375-1. Aus Gründen der einfacheren Administration sollte jedoch ein einheitliches Format für alle Modacom Chipkarten zur Anwendung kommen.

Die Maßangaben in Fig. 2 erfolgen in mm.

Die Chipkarte 1 wird bevorzugt mit einem extern getakteten 8 bit Micro-Controller in CMOS-Technik mit integriertem Halbleiterspeicher, aufgeteilt in RAM, ROM, und EEPROM ausgerüstet. Zur zeitgerechten Unterstützung der geforderten, extrem rechenintensiven Sicherheitsfunktionen (RSA-Verfahren, vgl. "Sicherheitsfunktionen") ist ein spezieller Co-Prozessor integriert. Eine besondere Security-Logik kontrolliert alle Speicherzugriffe und stellt die Integrität der Chipkartendaten gemäß der definierten Zugriffsbedingungen sicher.

Der Chip kommuniziert mit der Außenwelt über eine Schnittstelle gemäß dem internationalen Standard ISO/IEC 7816-3. An Stellen, wo diese Spezifikation unklar oder technisch überholt ist, werden geringe Modifikationen eingeführt, die aber in der Praxis keine Einschränkung der Kompatibilität darstellen und als Stand der Technik (z. B. in GSM) zu betrachten sind.

Es wird das ebenfalls in ISO/IEC 7816-3 standardisierte Übertragungsprotokoll T = 0 eingesetzt.

Architektur

Die Modacom Chipkarte erhält eine hierarchische Datenstruktur (vgl. Fig. 3).

Man unterscheidet von außen (nach Erfüllung der entsprechenden Sicherheitsstufe) zugreifbare Files sowie nur durch karteninterne Mechanismen verwaltete Daten. Für letztere stehen Schreib- oder Leseoperationen zur Außenwelt nicht zur Verfügung; es existieren lediglich spezielle, nur bei der Personalisierung nutzbare Einbring-Prozeduren.

Jedem Datenspeicher sind gewisse Sicherheitsstufen für Schreiben und Lesen zugeordnet, die durch Erfüllen der entsprechenden Zugriffsbedingung erreicht werden. Zwischen "Zugriff immer" und "Zugriff nie" befinden sich die Stufen AdLev1 (Produktion und Personalisierung), AdLev2 (autorisiertes administratives Terminal, etwa X13) und die Benutzer-Niveaus PIN und PUK.

Im Root-Directory befinden sich allgemeine, nicht Modacom-spezifische Informationen zur Karte und der enthaltenen Hardware. Sie werden bei der Produktion bzw. bei der Personalisierung (AdLev1) der Karte eingebracht und dienen danach der maschinenlesbaren Identifikation der Karte sowie einiger technischer Parameter. Die Daten sind unveränderlich, jedoch ohne Zugriffsschutz frei lesbar.

— Die ICC-ID ist die international eindeutige, 20-stellige Kartennummer, bestehend aus Länder- und Anwendungskennzahlen sowie der fortlaufenden Seriennummer.
— Die TIN (Technical Identification Number) liefert Informationen über den verwendeten Prozessortyp, die ROM Maske, sowie die Software-Version.
— Die Layout ID gibt dem lesenden Tool, z. B. Personalisierungssystem, eine Information über den Kartenkörper bezüglich Bedruck und Format. Diese administrativen Daten werden zur Produktionssteuerung im Personalisierungssystem benötigt.

Im Modacom Directory werden die anwendungsspezifischen Daten der Applikation Modacom bewahrt:

— Das Datenfeld Service Information dient der Identifikation von Spezialkarten, etwa für den Endgeräteservice. Modacom Terminals können bei Erkennen einer solchen Karte spezielle Wartungsfunktionalitäten (Monitorfunktionen, Debug-Mode, etc.) aktivieren, die mit einer Normalkarte nicht zugänglich sein sollen. Die Service Information wird bei der Personalisierung festgelegt und ist danach frei lesbar.
— Im Feld LLI befindet sich unveränderlich personalisiert die Teilnehmeridentität, gleichzeitig die Rufnummer des Teilnehmers im Modacom Netz. Als funktionswichtiges Datum ist sie mit der Sicherheitsstufe PIN geschützt.
— Der Home Node, eine zur optimierten Vermittlung wichtige Information, ist ebenfalls PIN geschützt, jedoch bei Bedarf auch nach der Personalisierung unter AdLev2 überschreibbar.
— Das Datenfeld Group ID enthält durch PIN geschützt, und nur von autorisierter Stelle veränderbar, eine Liste von Kennungen, die den Teilnehmer bestimmten Benutzergruppen zuordnet.
— Die Liste der Allowed PLMN enthält die vom Teilnehmer subskribierten Netze bei International Roaming. Nur für die hier enthaltenen Netzwerke besteht eine Teilnahmeberechtigung.
— Die Tabelle Network Information enthält für das Endgerät wichtige Parameter der existierenden Modacom Netze, wie z. B. Listen der möglichen Kanäle, erlaubte Sendeleistungen, etc.
— Die ICC Service Tabelle informiert das Endgerät über die in der Karte verfügbaren Services und Informationen. Gesetzte Bits zeigen an, ob etwa die PIN abstellbar ist, oder ob Network- oder MT-Configuration- Information überhaupt vorhanden und somit nutzbar sind. Wird bei der Personalisierung der Karte (AdLev1) festgelegt.
— Das Datenfeld MT Configuration enthält grundlegende Hardware Konfigurationsdaten für das

Mobile Terminal! (MT). Hier können z. B. Einstellungen für Power Management oder Interface und Communication Modes auf der Karte abgefegt werden. Nach erfolgreicher PIN Prüfung besteht freier Zugriff.

Diese Aufzählung ist nicht abschließend. Es können selbstverständlich- noch andere Informationen zusätzlich oder alternativ auf der Karte 1 enthalten sein.

Es existiert in der Karte 1 weiter eine Reihe von Datenfeldern, die intern verwaltet werden, d. h. ein Schreib- oder Lese-Zugriff über die Schnittstelle ist unmöglich. Enthaltene Daten werden über spezielle Routinen initialisiert oder verändert. Dazu gehören die Geheimschlüssel der Karte, die entweder im Rahmen der Personalisierung verschlüsselt in die Karte eingebracht werden (geheimer Authentifikationsschlüssel K_p, Benutzercodes PIN und PUK), oder von ihr selbst generiert werden (Session Key K_r).

Hinzu kommt die interne Datenstruktur Status, welche allgemeine Informationen über den momentanen Zustand der Karte (z. B. PIN- und PUK-Stati, Clock-Stop erlaubt, etc.) enthält.

PIN- und PUK Management

Die Modacom Chipkarte 1 verfügt über eine 4- bis 8-stellige Personal Identification Number (PIN), deren erfolgreiche Eingabe Voraussetzung zur Nutzung der Karte ist. Ein so erreichtes PIN-Recht bleibt bis zum Ende der aktuellen Kartensession, d. h. bis zum nächsten Power-Down oder Reset der Karte, erhalten.

Aus Sicherheitsgründen ist die Anzahl der möglichen aufeinander folgenden Fehlpräsentationen auf 3 beschränkt; selbstverständlich sind auch andere Sicherungsmechanismen denkbar. Danach ist die PIN-Prüfung gesperrt. Ein Entsperren ist mit dem 8-stelligen Personal Unblocking Key (PUK) möglich, welcher beispielsweise bis zu 10 Mal hintereinander falsch eingegeben werden kann. Danach ist die Karte endgültig gesperrt. Die PIN ist in der Regel vom Benutzer änderbar, der PUK jedoch nicht.

Die PIN-Prüfung ist seitens des Benutzers abstellbar, wozu jedoch die Kenntnis der PIN erforderlich ist. In diesem Falle sind Daten und Befehle der Karte so nutzbar, als wäre die PIN korrekt eingegeben worden.

PIN und PUK werden bei der Personalisierung in die Karte eingebracht und gleichzeitig in verdeckter Form ausgedruckt. Der Ausdruck (PIN/PUK-Brief) wird dem Benutzer zusammen mit der Karte ausgehändigt. Die Personalisierung von Karten mit abgeschalteter PIN-Prüfung ist möglich.

Befehlssatz

Der Befehlssatz der Modacom Chipkarte 1, d. h. die Menge der von der Karte ausführbaren Kommandos orientiert sich an den von der Karte zu erfüllenden Aufgaben:

— Administrative Funktionen: Hier stehen Funktionen zur Authentifikation auf Produktions- und Personalisierungsebene, zum Laden der Applikationssoftware, zum verschlüsselten Einbringen der Geheimschüssel, sowie verschiedene Prüfroutinen zur Verfügung.

— PIN-/PUK-Management: Entsprechend den Anforderungen sind Kommandos zum Verifizieren, Ändern, Ab-/Anstellen und Entsperren der PIN vorgesehen. Zur Ausführung von Funktionen, welche die PIN oder ihren Zustand ändern, wird die Präsentation der PIN vorausgesetzt.

— Sicherheitsfunktionen: Hierunter fallen Mechanismen für Authentifikation und Schlüsselaustausch sowie zur gesicherten Übertragung sensibler Daten (siehe Abschnitt 4).

— Speicherfunktionen: Selektieren von Datenstrukturen, Lesen und Schreiben der Inhalte. Es werden sowohl eindimensionale als auch listenartige Datenstrukturen unterstützt. Eine Funktion zum Ermitteln des Kartenstatus ist ebenfalls vorhanden.

Der vom Endgerät 2 initiierte Dialog mit der Chipkarte 1 setzt sich aus einer grundsätzlich beliebigen (jedoch durch anwendungstechnische Notwendigkeiten z. T. vorgegebenen) Aneinanderreihung der verfügbaren Funktionen zusammen. Die Kontrolle über die Chipkarte 1 liegt damit jederzeit beim Endgerät 2, welches flexibel und wahlfrei auf die Karte zugreifen kann. Zu jedem empfangenen Kommando generiert die Karte eine Quittungsinformation, die dem Endgerät eine Information über den aktuellen Verarbeitungszustand anzeigt (z. B. Befehl erfolgreich beendet, PIN falsch, Kommando unbekannt etc.)

Sicherheitsfunktionen

Die Einführung der Chipcarte 1 in das Mobilfunksystem Modacom geschieht mit dem Ziel, das vorhandene Sicherheitsniveau nicht zu beeinträchtigen und nach Möglichkeit sogar zu steigern.

Die Chipkarte 1 bedingt eine zusätzlichen Schnittstelle, über welche sensible Daten übertragen werden. Diese Chipkarte und damit die Schnittstelle ist mehr oder weniger frei zugänglich, und somit gegen Angriffe wie Abhören, Verfälschen oder Vortäuschen falscher Identitäten prinzipiell nicht abzusichern.

Um solche Angriffe nicht zum Erfolg kommen zu lassen und somit entscheidende Sicherheit nicht zu verlieren, werden spezielle kryptografische Mechanismen vorgesehen, welche die nachweisbare Echtheit der übertragenen Daten im Rahmen der Grundgüte der verwendeten Verfahren (welche allerdings als sehr hoch einzuschätzen ist) sicherstellen.

In gleicher Weise ist die Datensicherheit der Chipkarte 1 nach heutigem Kenntnisstand als äußerst hoch anzusehen. Die vorgesehene Kartentechnologie bietet extremen Schutz gegen alle denkbaren physikalischen und logischen Angriffe auf Integrität und Vertraulichkeit der enthaltenen Daten. Die zur Anwendung in Modacom vorgeschlagene Klasse der Krypto-Prozessoren ist auf sicherheitskritische Anwendungen spezialisiert und kann als Stand der Technik angesehen werden.

Zu der angestrebten Sicherheit des Subsystems Endgerät 2 — Karte 1 gehört jedoch auch die Sicherheit der einmal gelesenen Kartendaten im Modacom Endgerät 2. Die Anforderungen gegen Verfälschen oder Vortäuschen dieser Informationen, etwa durch Eingriff in das Endgerät, erfordern ebenfalls besondere Design-Maßnahmen.

Wichtig ist, daß außerhalb des Terminals im System Modacom ggf. vorhandene Sicherheitsrisiken durch den Einsatz der Chipkarte 1 weder behoben noch kompensiert werden. Setzt man eine ausreichende Sicherheit der Endgeräte 2 voraus, so kann jedoch gegenüber dem Zustand ohne Chipkarte 1 von einer spezifisch erhöhten

Sicherheit gesprochen werden, denn:

— Die Verwahrung der Daten in der Chipkarte ist allgemein sicherer als in der Hardware des Endgerätes.
— Der verantwortliche Umgang mit sensiblen Daten liegt komplett beim Netzbetreiber. Prinzipiell mit Sicherheitsnachteilen behaftete Programmier- und Editierwerkzeuge existieren nicht mehr.
— Durch (optionale) Verwendung der PIN-Prüfung existiert ein Schutz des Teilnehmers gegen unerlaubte Benutzung oder Diebstahl der Karte 1 allein oder des Endgerätes 2 zusammen mit der Karte.

Im folgenden werden die zur Erreichung des angestrebten Sicherheitsniveaus notwendigen Prozeduren erläutert.

Authentifikation

Die Chipkarte 1 muß in der Lage sein, ihre Echtheit (Authentizität) jederzeit zweifelsfrei gegenüber dem Terminal/Endgerät 2 zu beweisen. Da die Programmierung der Endgeräte mit individuellen Schlüsseln nicht in Betracht kommt, können hier nur asymmetrische Kryptoverfahren angewendet werden, bei denen die Karten einen geheimen Schlüssel K_s, die Endgeräte jedoch einen öffentlichen Schlüssel K_p tragen. Nur wenn K_s und K_p zusammenpassen, verläuft die Authentifikation erfolgreich. Es ist nicht möglich, vom öffentlichen Schlüssel auf den geheimen Schlüssel zurückzuschließen und so das Verfahren zu brechen.

In der praktischen Realisierung wird das RSA-Verfahren (Schlüssellänge 512 bit) vorgeschlagen, welches als Standard in vergleichbaren Anforderungen anzusehen ist.

Die Sicherheit gründet sich auf hierbei vollkommen auf die Vertraulichkeit des geheimen Schlüssels K_s, der in allen Modacom Chipkarten 1 enthalten ist. Das heißt, wird jemals — auf welche Weise auch immer — dieser Schlüssel bekannt, so sind alle Karten in gleicher Weise betroffen. Um den Schaden in diesem theoretischen Fall zu begrenzen, werden Schlüsselpaare $K_s(i)$ und $K_p(i)$, mit $i = 1, 2, \ldots, 10$ vorgesehen, die gleichverteilt in die Chipkarten eingebracht werden. Als Schlüsselindex i dient die letzte Stelle der Karten-Seriennummer (vorletzte Stelle der ICC-ID), die gleichzeitig eine äußere Identifizierung des Schlüsselindex ermöglicht.

Damit weiterhin Endgeräte 2 und Karten 1 beliebig austauschbar sind, müssen Endgeräte 2 alle 10 öffentlichen Schlüssel kennen, von denen der passende anhand des Schlüsselindex ausgewählt wird. Durch diese Maßnahme verringert sich das beschriebene Restrisiko bei Bekanntwerden eines Schlüssels K_s auf 1/10tel.

Der gesamte Vorgang der Authentifikation gestaltet sich wie folgt (**Fig. 4**):
Das Endgerät 2 liest die ICC-ID aus der Karte 1. Anhand der letzten Ziffer wird der Schlüsselindex ermittelt; $K_p(i)$ steht somit fest. Anschließend generiert das Endgerät 2 eine Zufallszahl, welche im Rahmen des Authentifikations-Befehls zur Karte 1 übertragen wird. Die Karte verschlüsselt die übergebene Zufallszahl mit ihrem geheimen Schlüssel $K_s(i)$ zu X, und antwortet dies dem Endgerät. Hier wird mit $K_p(i)$ zurückentschlüsselt und das Ergebnis mit der anfangs erzeugten Zufallszahl verglichen. Übereinstimmung beweist zusammenpassende Schlüssel und damit die Echtheit der Karte.

Selbstverständlich sind auch beliebige andere Verfahren einsetzbar.

Sichere Datenübertragung durch MAC Bildung

Die Authentifikation liefert einen Beweis über die Echtheit der präsentierten Chipkarte 1, jedoch nicht über die Echtheit der nachfolgend vom Endgerät 2 empfangenen Daten — diese könnten ja auf der Schnittstelle manipuliert worden sein.

Zur Absicherung des Datentransfers wird ein Prüfsummen-Verfahren verwendet, siehe **Fig. 5**. Die zu übertragenden Daten werden von der Chipkarte 1 von einem Ein-Weg-Algorithmus (DES im Cipher Block Chaining Mode) mit dem geheimen Schlüssel K_r verschlüsselt. Das Ergebnis wird als Prüfsumme (MAC, Message Authentifikation Codes zusammen mit den Daten zum Endgerät 2 übertragen. Hier wird der Vorgang wiederholt und durch MAC-Vergleich die Echtheit der Daten überprüft.

Der hierzu auf beiden Seiten notwendige Geheimschlüssel K_r wird in einer vorgeschalteten Prozedur vom Endgerät 2 erzeugt und der Karte 1 mitgeteilt, vgl. **Fig. 6**. Per Zufallsgenerator wird der K_r im Endgerät generiert und RSA-verschlüsselt zur Karte übertragen. Nach der Entschlüsselung steht der Schlüssel K_r auf beiden Seiten zur Verfügung.

Der Schlüsselaustausch wird in jeder Kartensession mindestens einmal, z. B. im Rahmen der Authentifikation, automatisch durchgeführt. Damit wird sichergestellt, daß nach jeder Kartenaktivierung -Einschalten des Endgerätes. Karte stecken oder Reset) ein unvorhersagbarer Schlüssel zur Verfügung steht.

Die durch MAC abgesicherte Übertragung wird für alle identifizierenden Chipkartendaten (LLI, Home Node, Group ID) durchgeführt, welche naturgemäß gegenüber Verfälschung oder Vortäuschung besonders zu schützen sind.

Sicherheitsrelevante Endgeräteanforderungen

Die beschriebenen Funktionalitäten setzen im Endgerät 2 entsprechende Unterstützung voraus, d. h. es müssen Möglichkeiten zur Zufallszahlengenerierung und zur zeitgerechten RSA-Berechnung vorhanden sein. Die Anforderungen sind analog zu denen an die Chipkarte 1.

Der Zusammenspiel des Modacom Endgerätes 2 mit den beschriebenen Sicherheitsfunktionen der Karte 1 wird in der Praxis einer Kartensession etwa wie folgt ablaufen:

(1) Die Kartenschnittstelle wird aktiviert und ein Power-on Reset durchgeführt. Bei eingeschalteter PIN Prüfung sind nur die in **Fig. 3** als "immer lesbar" gekennzeichneten Datenfelder zugreifbar. Das Endgerät 2 ermittelt den PIN Status und bittet die Applikation (den Benutzer) um Übergabe der PIN. Der Geheimcode wird an die Karte 1 übergeben und die Verifikation durchgeführt. Ist die PIN korrekt, wird das entsprechende Zugriffsrecht vergeben. Bei ausgeschalteter PIN Prüfung ist dieser Zustand automatisch nach dem Reset vorhanden.
(2) Das Endgerät liest die ICC-ID und führt die Authentifikation und den Schlüsselaustausch wie beschrieben durch. Ist die Karte echt, befinden sich anschließend gleiche Sessionkeys K_r in Karte und Endgerät.

(3) Es kann nun auf alle PIN geschützten Informationen wahlfrei zugegriffen werden. Die Erzeugung und Übertragung des MAC erfolgt bei sicherheitskritischen Daten automatisch.

Es ist dabei vorausgesetzt, daß die Applikation im Endgerät sich entsprechend den Anforderungen verhält, d. h. die notwendigen Schritte und Reihenfolgen auch durchführt. Bei sicherheitskritischen Abweichungen, z. B. unterlassene PIN-Prüfung, wird die Karte ihre Funktion sperren — zumindest sind aber die von ihr erhaltenen Daten ungültig.

Es lassen sich einige weitere sicherheitsrelevante Bedingungen an das Modacom Endgerät 2 formulieren:

— Es darf keine nicht-flüchtige Speicherung von Kartendaten erfolgen, d. h. nach Ausschalten oder Reset des Terminals dürfen diese im Endgerät nicht mehr vorhanden sein.
— Die Entnahme der Chipkarte während des Betriebs ist sicher zu erkennen und muß zum Abbruch einer bestehenden Verbindung und zum Löschen aller Kartendaten aus den Speichern des Endgerätes führen. Eine geeignete Möglichkeit dazu wäre etwa eine zyklisch durchgeführte Authentifikation.
— Die Übertragungswege identifizierender Kartendaten sind innerhalb des Endgerätes gegen Verfälschung und Vortäuschung ausreichend abzusichern.
— Das Endgerät muß der Applikation eine Schnittstelle zur Übertragung der PIN-Funktionen bereitstellen. (Die Nutzung ist für die Applikation optional, wenn die PIN-Prüfung in der Karte abgestellt ist.)

Fazit

Das vorliegende Dokument liefert eine realistische Möglichkeit zur Einführung einer Chipkarte in das Mobilfunksystem Modacom. Die technische Lösung erreicht die angestrebten Vorteile sicher. Durch weitestgehende Berücksichtigung bereits vorhandener Konzepte und Verfahrensweisen sowie durch die Verwendung internationaler Standards werden technische Risiken ausgeschlossen. Das Ergebnis ist eine Chipkartenapplikation, welche dem mobilen Datenfunk entscheidende neue Impulse geben kann.

Patentansprüche

1. Verfahren zur Nutzeridentifikation und -authentifikation bei Datenfunk-Verbindungen, **dadurch gekennzeichnet**, daß die zur Nutzeridentifikation erforderlichen Daten auf einem gesonderten Datenträger (1) getrennt von einem Endgerät (2) abgelegt werden.
2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die Nutzeridentifikation und -authentifikation durch Kommunikation zwischen Datenträger (1) und Endgerät (2) durchgeführt wird.
3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die Nutzeridentifikation und -authentifikation durch Kommunikation zwischen Datenträger (1) und einer endgerätunabhängigen Applikation (3) durchgeführt wird.
4. Verfahren nach einem der vorhergehenden Ansprüche dadurch gekennzeichnet, daß bei der Verständigung zwischen Datenträger (1) und Endgerät (2) bzw. Datenträger (1) und Applikation (3) mindestens ein kryptographisches Verfahren zur Datenverschlüsselung eingesetzt wird.
5. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die auf dem Datenträger (1) enthaltenen Daten in von Benutzer änderbare, lesbare und nicht-lesbare Daten eingeteilt werden.
6. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die auf dem Datenträger (1) enthaltenen Daten über mindestens einen vom Benutzer einzugebenden Code gesichert werden.
7. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die Nutzeridentifikation und -authentifikation bei längerem Datenaustausch oder physischem Kontakt zwischen Datenträger (1) und Endgerät (2) in bestimmten Zeitabständen wiederholt wird.
8. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß bei einer Entnahme des Datenträgers (1) aus dem Endgerät (2) während des Betriebs eine bestehende Verbindung abgebrochen wird.
9. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die von dem Datenträger (1) erhaltenen Daten im Endgerät (2) sowie gegebenenfalls von der Applikation (3) nur flüchtig gespeichert werden.
10. Datenträger zur Durchführung des Verfahrens nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß der Datenträger als Chipkarte (1) ausgebildet ist.
11. Datenträger nach Anspruch 10, dadurch gekennzeichnet, daß der Datenträger (1) einen Mikro-Controller und einen EEPROM-Speicher aufweist.
12. Datenträger nach Anspruch 11, dadurch gekennzeichnet, daß der Datenträger (1) einen vom Benutzer frei belegbaren Speicherabschnitt aufweist.
13. Endgerät zur Durchführung des Verfahrens nach einem der Ansprüche 1—7, dadurch gekennzeichnet, daß die im Endgerät (2) vorhandenen Übertragungswege für die nutzerspezifischen Daten abgesichert sind.
14. Endgerät nach Anspruch 13, dadurch gekennzeichnet, daß das Endgerät (2) mit flüchtigen und nicht-flüchtigen Speicherplätze versehen ist.

Hierzu 3 Seite(n) Zeichnungen

Nummer: DE 195 27 715 A1
Int. Cl.[6]: H 04 L 9/32
Offenlegungstag: 6. Februar 1997

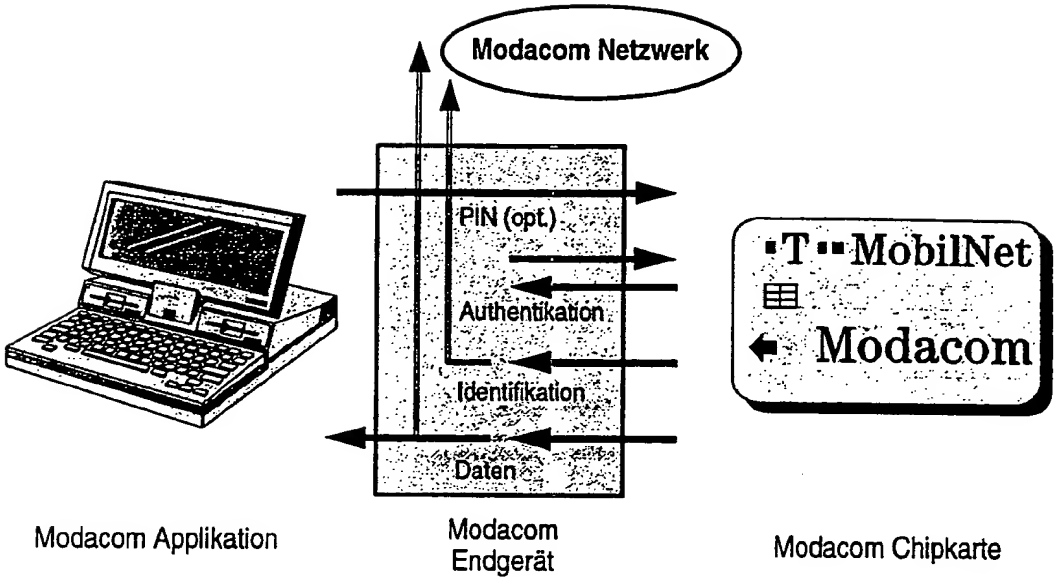

Fig. 1

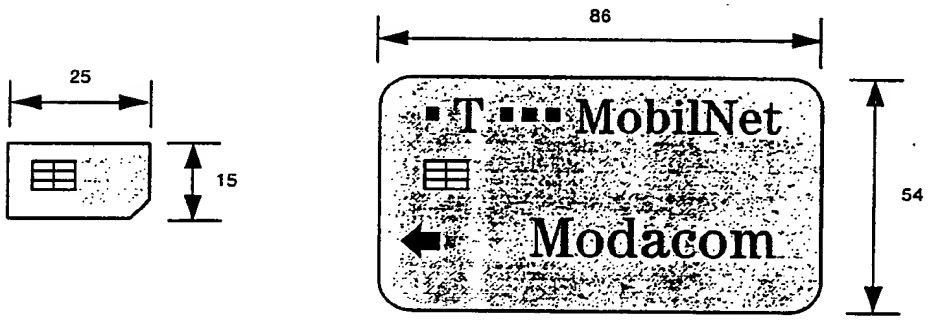

Fig. 2

Nummer: DE 195 27 715 A1
Int. Cl.[6]: H 04 L 9/32
Offenlegungstag: 6. Februar 1997

Datenstruktur	lesen	schreiben
von außen zugreifbar		
Root		
ICC-ID	immer	AdLev1
TIN	immer	AdLev1
Layout ID	immer	AdLev1
Modacom		
Service Information	immer	AdLev1
LLI	PIN	AdLev1
Home Node	PIN	AdLev1/2
Group ID	PIN	AdLev1/2
Allowed PLMN	PIN	AdLev1/2
Network Information	PIN	AdLev1/2
ICC Service Table	PIN	AdLev1
MT Configuration	PIN	PIN
...	...	...
intern verwaltet		
Secret Key Ks	nie	nie
Session Key Kr	nie	nie
Secret Keys PIN + PUK	nie	nie
Status	nie	nie

Fig. 3

Nummer: DE 195 27 715 A1
Int. Cl.[6]: H 04 L 9/32
Offenlegungstag: 6. Februar 1997

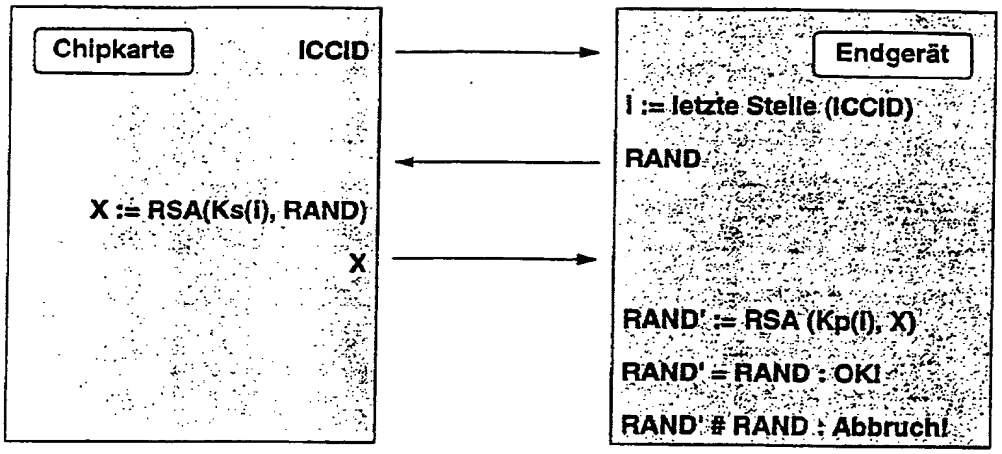

Fig. 4

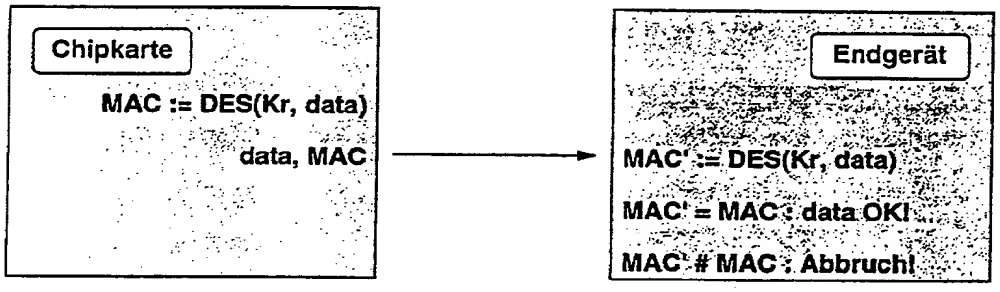

Fig. 5

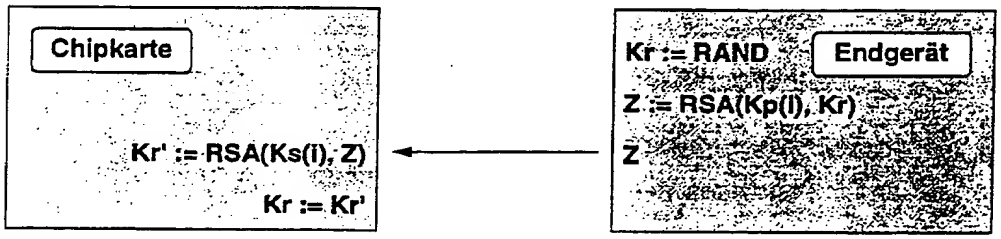

Fig. 6